POINTS FOR CONSIDERATION RELATIVE TO A NATIONAL POLICY ON DAMAGE ASSESSMENTS

I. Background

This paper represents a preliminary effort to examine the damage assessment process to determine what, if anything, could be done to optimize the process. Rather than attempting a definitive study of the subject, an effort has been made to identify issues which require further exploration. Positions taken on these issues will determine what additional work is necessary in this area. (U)

As a point of departure it is useful to note that a national policy on damage assessments is articulated in Information Security Oversight Office (ISOO) Directive No. 1. (32 CFR Part 2001). This Directive, which is binding on the various departments and agencies, was promulgated pursuant to authority granted the Director of that Office by the President in Section 5.2 of Executive Order 12356 (April 6, 1982). The Directive states in Section 2001.47:

> Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to an official designated for this purpose by the person's agency or organization. The agency that originated the information shall be notified of the loss or possible compromise so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise. The agency under whose cognizance the loss or possible compromise occurred shall initiate an inquiry to (a) determine cause, (b) place responsibility, and (c) take corrective measures and appropriate administrative, disciplinary, or legal action. (U)

The ISOO Directive attacks the problems of loss or compromise of classified information along two dimensions. First, the originating agency, that is the agency which owns the material, is charged with the responsibility to conduct a damage assessment and to take appropriate measures to negate or minimize any adverse effect of the compromise. Second, the agency with responsibility for the loss or compromise is required to

determine how the loss occurred, to take corrective and remedial steps to prevent the problem from recurring and to take administrative, disciplinary or legal action against those responsible for the loss. (U)

In discussing damage assessments, an expansive definition of the term, and of the process, has been adopted. When an incident occurs, it would be expected that a four-step process would begin:

> First, a preliminary inquiry would be undertaken to determine whether there has been a compromise of classified information. If a compromise has occurred, then a preliminary judgment must be made as to whether the compromise could reasonably be expected to cause damage to the national security.
>
> Second, if a compromise of classified information has occurred and the probability of damage to the national security cannot be discounted, then an inventory of the classified information involved would be prepared and the impact of the compromise on the national security would be evaluated.
>
> Third, if it is determined that the compromise could have a significant impact on the national security, appropriate countermeasures to negate or minimize the effect of the compromise would be identified.
>
> Fourth, remedial or corrective action would be specified. An attempt would be made to identify the person(s) responsible for the compromise and administrative, disciplinary or legal action would be proposed to deal with the situation. Even when it is not possible to identify the person responsible for the compromise, it may be possible to examine what went wrong. If existing procedures are deemed adequate, but implementation has been sloppy, employee notices or additional training may be appropriate. If systemic problems or gaps in regulations or procedures are identified, then more extensive corrective action would be required. (U)

II. Issues

A. National Level Guidance With Respect To Damage Assessments -- Investigative Triggers

There was near unanimity that a full-blown damage assessment would not be appropriate in every case and inflexible requirements would be counterproductive. If, for

example, a safe were left open in a controlled facility and discovered by a security guard soon afterward, cataloging all of the items in the safe and assessing the national security impact of the possible compromise may not be necessary. On the other hand, even in the above circumstance, if the open safe contained a master list of safe combinations, it would be prudent to change all of the safe combinations. Even at the other end of the spectrum discretion is desirable. If, for example, a diplomatic pouch containing large sums of money were broken into and the money taken while other material and documents were left untouched, a damage assessment might not be required unless the theft were considered to be a cover for the photographing of the documents. (U)

Despite the unanimity that discretion must be built into the system, there was a division of opinion as to whether there should be any national level guidance. It was suggested that when specialized intelligence equipment or classified military equipment is lost, a human source or a technical collection system is jeopardized, a diplomatic pouch containing classified information is lost, a secure facility is penetrated, or espionage occurs, a full damage assessment should be required unless the agency head or designee expressly determines that this is not necessary. (U)

B. Improved Quality Control

At present there is no way of evaluating, outside of existing chains of command, whether damage assessments when done are well done. Although there is no clear evidence that damage assessments are deficient, there is considerable question about the extent to which they are merely descriptive rather than analytical and prescriptive. There is, moreover, no current ability to hold up a particularly good damage assessment as a model for others to emulate. There is always the suspicion, however ill-founded, that damage assessments prepared by the components most intimately involved are self-serving documents which may inflate or devalue impacts or which may mask or minimize problems, procedural inadequacies or poor personnel or program management. (U)

There was a clear consensus, however, that agencies should not lose control of the damage assessment process. Each agency should conduct its own damage assessment and should be free to structure an investigative framework which adequately reflects the realities of that agency. On the other hand, there was less clarity as to whether adequate quality control could be assured at the program manager level or whether a broader agency perspective would be helpful. (U)

It was suggested that it might be useful to establish a separate mechanism within each agency to ensure the timeliness and quality of damage assessments. There was some feeling that a separate mechanism which focused exclusively on the quality and timeliness of such assessments could in time appreciably enhance the value of such asssessments to each agency. The specific mechanism would vary according to the unique configuration and structure of each agency. Each quality control mechanism, however, would be empowered to make recommendations involving specific damage assessments to the extent that discrete deficiencies are found. In addition, by analyzing large numbers of damage assessments over time, the quality control mechanism could make recommendations concerning improvement in the methodology and approach taken in putting together such assessments. For example, it could ensure that the substantive and technical expertise represented by the operational components whose information was compromised and the specialized knowledge of the analytical components able to assess the impact of the compromise had been adequately utilized. In addition, it could ensure that security, counterintelligence and inspection or program audit perspectives had been included. It also could review whether damage assessments could better be conducted by individuals or teams specially designated to examine a particular leak or by units with a permanent membership. It could assess whether organizational changes were needed in order to spur new thinking or whether there was a need to create or improve institutional memory and level of experience in examining compromises. (U)

C. Assessment Implementation

The most significant parts of a damage assessment are its forward looking aspects. Obviously countermeasure recommendations help to make a bad situation better. The remedial or corrective steps which are designed to determine cause, to place responsibility, to recommend administrative, disciplinary or legal action, or to implement policy and procedural changes are critically important. There is considerable question, however, about the extent to which ar recommendations which are made are actually implemented. It is suggested, therefore, that a tickler or review system be established to revisit damage assessments after a three or six-month interval to determine whether it is still "busine as usual," or whether the changes which have been made are really working and are adequate to prevent a recurrence. (

Opponents suggest that under current procedures, the chain of command is responsible for implementing corrective or remedial measures and that there is no need for any chan in the system. Proponents suggest that under the current system the status of damage assessments, the status of various recommended courses of action, or even whether the case has been closed from an administrative, disciplinary (

legal point of view often is unclear. In sum, proponents suggest that there is such a variety and diversity of disclosures which are reported through so many different chains of command that appropriate coordination and necessary feedback very often is lacking. (U)

D. Sharing of Information

The present damage assessment system is deficient because of the paucity of mechanisms by which lessons learned can be shared. There is some dissatisfaction with the current, informal, ad hoc system of exchanging information. It is recognized that there is a natural concern about airing "dirty linen" in public. There are justifiable concerns about security, particularly when compartmented or "bigoted" programs are involved. There also is the view that many of the remedial measures proposed may be program or organization specific with little relevance outside a very narrow circle. To be sure there may be natural boundaries beyond which the costs of sharing information may exceed the benefits. However, even if it is argued that it is not useful to share information outside these natural boundaries, greater sharing of information than currently is the case should be encouraged. (U)

It is suggested that there is a military hardware or weapons system grouping. There is an Intelligence Community and within that there is an SCI Community. At least within each of these groupings information can be pooled. Mistakes which have been made on one program or compartment may later be made by individuals working on another program or in another compartment. It often is possible to generalize from remedial measures taken in one program so that other program managers can benefit. More to the point, this can be done without touching upon the particularly sensitive information. In the Boyce-Lee case, for example, it was not necessary to discuss the specific company, or the specific intelligence system involved in order to share with other program managers the utility of the two person rule or the desirability of instituting an industrial polygraph program. The issue here is whether there should be some national level guidance which encourages or mandates sharing of information or whether the present system, which largely leaves sharing of information to each program manager, is adequate. (U)

Currently, the Air Force has a newsletter (published 3 to 4 times a year) that synopsizes various cases involving unauthorized disclosures of SCI which the Air Force determines to be of general applicability and interest. The Air Force disseminates this newsletter throughout the SCI Community, both inside and outside the Department of Defense. By means of this newsletter the SCI Community is given the benefit of Air Force experience in a variety of

unauthorized disclosure cases and is able to apply any preventive measures necessary to safeguard against a repetition elsewhere in the Community of the circumstances which led to particular unauthorized disclosures. (U)

It is suggested that the Air Force newsletter serve as a model for other newsletters which would address the needs and interests of various appropriate communities. The SECOM could publish such a newsletter regarding cases of broad interest to the Intelligence Community, in general, or to the SCI Community, in particular. Similarly, the ISOO could be tasked with publishing such a newsletter concerning unauthorized disclosures within various communities of interest that relate to the world of collateral classified information. It is significant to note that DCID 1/19, as currently revised, provides for sharing with the SECOM and the DCI summaries of investigations and related actions in cases involving significant compromises. (U)

E. The Data Base

Another area of discussion centered upon the proposed establishment of an unauthorized disclosure data base. It appears that the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) are moving inexorably toward establishing a data base which would contain all information relating to unauthorized disclosures reported to them. DOJ strongly believes that such a data base would be useful to it and to the FBI in getting an analytical handle on the problem of unauthorized disclosures. That is to say, DOJ is interested in analyzing large numbers of unauthorized disclosures to determine if there are any significant commonalities, patterns, or trends that emerge from the data that would aid the FBI in its investigations of such matters. With this DOJ initiative on the horizon, it is believed that an even broader data base would be useful to agencies within various appropriate communities. (U)

Under a proposal for a broad data base, the participating agencies would, above some pre-determined level of triviality, contribute information on unauthorized disclosures to a central system, whether or not the disclosures were reported to DOJ. The greatest concern with the establishment of such a system was that in order for the system to be effective, it would require that all relevant information regarding unauthorized disclosures be fed into the system. This might include very sensitive information. (U)

The concern expressed fails to take into account the fact that other very sensitive data bases already exist with appropriate safeguards. For example, there is a Government-wide register of human intelligence sources which, though extremely sensitive, provides an invaluable reservoir of

information that enables the [illegible] efficiently and effectively conduct its assessment and recruiting activities. To avoid widespread dissemination of sensitive information relating to unauthorized disclosures, the proposed system could be similar in design to the 4C System, which is intended to contain an equally sensitive data base of all SCI accesses for all SCI programs. Only a limited number of people would have access to the proposed system and an even more limited number would have access to the particularly sensitive information in such a system. (S)

Hopefully, as a comprehensive analytical platform, such a data base could ultimately become an important diagnostic tool for the participating agencies. The data base would provide useful information concerning the specific types of information being disclosed, any correlation between types of disclosures and government processes, any correlation between types of disclosures and media representatives, and past disinformation programs. The information gained from the analysis of such a data base would assist in evaluating existing security practices and developing any new ones determined to be necessary. It would assist in developing models of the various types of inadvertent disclosures. It would assist in concentrating security resources in specific areas where the risk of disclosure is high. It would quickly identify old releases, isolate chronic leakers, develop countermeasures for disinformation and deception programs. Finally, it may be useful in predicting future trends with respect to unauthorized disclosures so that anticipatory countermeasures may be implemented. (S)

F. Regulations

As a final point it was noted that it would be useful for those agencies which have not yet issued regulations implementing ISOO Directive No. 1 to do so. In addition, if any of the above recommendations are adopted, they might be included in existing or new regulations. (U)